DRN-5112599

The complaint

A company, which I'll refer to as C, complains that GPUK LLP (trading as Global Payments (GP)) has charged it excessive Payment Card Industry Data Security Standard (PCI DSS) charges, which it would like refunded.

Mrs C, a director of C, brings the complaint on C's behalf.

An employee of C has represented C in its complaint. However, I will refer to all comments and submissions received as being from C.

What happened

The circumstances of this complaint are familiar to both parties so I will only summarise here:

- As part of C's agreement with GP, C is obliged to validate with GP its compliance to the PCI DSS; and, if compliance is not validated, GP will charge C a PCI DSS fee per transaction until compliance is validated.
- In July 2023, GP sent C a reminder letter, notifying C that its validation would be expiring in September.
- In August 2023, GP sent C three email reminders prompting it to take action.
- C's validation expired in September 2023, and wasn't re-validated until the end of January 2024.
- In September 2023, after C's validation had expired, GP sent C four further emails, stating clearly that non-compliance fees would start from 30 September.
- C complained. It acknowledged that PCI DSS charges were due for the period prior to its re-validation, but complained about the level of those charges, which it said were excessive and unjustified. C also said that GP had not been clear about the charges and felt they are hidden deliberately.
- As a gesture of goodwill, GP refunded the PCI DSS fees paid by C in January and February 2024.

Our investigator looked into things and found that GP had applied non-compliance PCI DSS fees to C's account in line with the terms of its agreement with C. He noted the reminders sent by letter and email to C before compliance lapsed, and the further emails in September. He said that GP had highlighted the importance of PCI DSS compliance and validation in the paperwork provided to C when it first signed up with GP, and said that GP had good reason to encourage compliance. He found that the level of non-compliance fee charged by GP was not disproportionate to GP's genuine interest in ensuring C maintained its PCI DSS compliance.

C did not agree so the matter has been passed to me to resolve. In its response to our investigator, C raised several points, which I have considered in my decision below.

What I've decided – and why

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

Level and purpose of the non-compliance fee

C has said that it doesn't dispute there should be a penalty but that the amount charged by GP was unreasonable and disproportionate. C has stated that in some months the PCI DSS charge was more than its total card processing charge.

Compliance with the PCI DSS is clearly very important, and I believe it is reasonable for GP to take steps to ensure its merchants remain compliant. Therefore, while GP's per-transaction PCI DSS non-compliance fee is high, I cannot say that this is unfair given its intended purpose to encourage compliance.

C has also said that, although the purpose of the fee might be to encourage compliance, the box-ticking exercise doesn't actually prove compliance. C has said that it has been compliant at all times with the PCI DSS, while GP's process of validation seems intended only to remove liability for GP if things go wrong.

It is not for me to comment on the full package of controls GP or the card schemes should apply to ensure merchants are PCI DSS compliant, or the evidence they should gather to demonstrate compliance. In the circumstances of this complaint, the question for me to consider is about the reasonableness of the non-compliance fee, and I cannot say that the fee charged by GP to C to encourage PCI DSS compliance was unreasonable.

Transparency of the non-compliance fee and notification given

C has said that the PCI DSS non-compliance fee was never made clear in GP's communication. It said that the details about this fee were not written in its contract with GP but accessed through an electronic link. C has also said that at no point did GP clearly state the amount that would be charged, including in the emails leading up to its non-compliance.

I've looked through the information which would have been provided to C when it signed up with GP and seen that the merchant's PCI DSS responsibilities are shown clearly in both the Terms of Service, which govern the agreement between GP and the merchant, and the Know your Risks leaflet.

For example, the Know your Risks leaflet states:

> *If you don't validate your compliance, we will apply a monthly non-compliance charge of £0.15 for each sale transaction we process on your behalf, subject to a minimum monthly charge of £75.00 per merchant ID, for each month you remain non-compliant. The charge will be applied the following month in arrears and is not refundable.*
> *You can easily avoid this monthly non-compliance charge by achieving and maintaining PCI DSS compliance.*

And the Merchant Operating Instructions state:

> *If you don't validate your compliance, you'll be subject to monthly non-compliance charges that are charged in arrears and are non- refundable. These non-compliance charges will continue until you achieve PCI DSS compliance. Details of the non-compliance charges can be found on www.globalfortress.co.uk.*

Even though the level of the PCI DSS non-compliance fee is not stated in the agreement itself, I think it is stated clearly in this other documentation provided to the customer.

I do not think that GP was obliged to remind C of the level of fees it would incur when notifying it of its imminent non-compliance.

I also note that GP has provided evidence to show that the amount actually charged to C for PCI DSS non-compliance was stated clearly on each invoice.

For these reasons, I think GP made reasonable efforts to set out the fees C would incur for PCI DSS non-compliance, and it was reasonable in the circumstances for GP to charge this fee in accordance with its agreement with C.

C has also said that it did not receive GP's emails but that demonstrating this as a small business is incredibly hard against a business the size of GP. C has also queried why GP didn't phone C to notify it of the high charges.

I've seen the emails sent to C by GP in August and September 2023, all of which are addressed to the same email address we have been using to communicate with C. On balance, I think it most likely that these emails were sent by GP, which, together with the letter sent in July 2023, indicates to me that it made substantial efforts to notify C of C's impending non-compliance. I don't think GP acted unreasonably in not also phoning C.

Summary

Overall, it appears to me that GP made reasonable efforts upfront when C became a customer of GP to explain the charges C would incur if it did not validate and maintain the validation for C's PCI DSS compliance. In the summer of 2023, GP also made reasonable efforts to notify C that its validation would be expiring and that C needed to take action to avoid these charges. Subsequently, GP informed C every month of the PCI DSS non-compliance fees it was being charged.

While I acknowledge that the level of PCI DSS fees charged to C by GP was high, I cannot say that the amount was excessive or disproportionate given its purpose to encourage compliance. It is not for me to comment on what other measures GP should take to monitor the compliance of its customers.

I have a lot of sympathy for Mrs C and the situation her business has found itself in. In a busy business with many card transactions being processed by GP, the per-transaction non-compliance PCI DSS fee charged by GP quickly added up into a substantial total amount. However, for the reasons set out above, I can't say that GP has done anything wrong, so I won't be asking it to take any further action.

My final decision

For the reasons set out above, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask C to accept or reject my decision before 5 March 2025.

Andy Wright
Ombudsman